Reconfiguration analysis of carrier security system for IPv6

Jingjing Zhang[1], Chao Wang[2], Bin Chen[1], Xiaobing Fu[2]

1. Jiangxi Branch of China Telecom Corporation Limited, Nanchang 330029, China

2.Jiangxi Branch of National Internet Security Administration Center, Nanchang 330038, China

Abstract: With the continuous development of the Internet, IPv6 planning and deployment has become the current "accelerate the construction of network power, to win the future international competition of new advantages" an urgent requirement, and the current security system reconstruction in the implementation of IPv6 planning and deployment plan has a very important practical promotion significance. However, we should pay attention to one point is that compared with the Internet construction and operation and maintenance, the operator IPv6 network construction and its security operation and maintenance is a certain difference. Therefore, based on the background of the new era, it is very necessary to actively explore the path of IPv6 oriented carrier security system reconstruction planning. Based on this, this paper first describes the application advantages of IPv6, and briefly analyzes the status quo of the carrier security system, and discusses the reconstruction direction and planning of the IPv6 oriented carrier security system, for reference only.

Key words: Internet; IPv6; Carriers; Safety guarantee system; Planning reconstruction

1. Application advantages of IPv6

IPv6 (Internet Protocol Version 6) is a more efficient and sustainable network. The IPv6 protocol can provide people with a very large number of IP addresses, so compared to IPv4 networks, IPv6 networks are more efficient, less expensive, and have some sustainable development. Its application advantages mainly include the following points:

1.1 IPv6 can realize the sustainable development of the Internet

From the current point of view, the length of IPv6 network IP address has increased to 128b, a total of about 3.4×1038 IP address resources, while the total number of IPv4 address resources is about 4.3 billion, which shows the large number of IPv6 address resources. Therefore, the large number of IPv6 address resources can well ensure that the Internet will not hinder its development due to the lack of geological resources in the next few hundred years.

1.2 IPv6 can support automated configuration

IPv6 protocol can support stateless address automatic configuration, when the IPv6 terminal network, it can automatically obtain the corresponding IP address, without manual configuration can be used, can really achieve "plug and play", which has great significance for the improvement of Internet management efficiency.

1.3 IPv6 has stronger mobility characteristics

Mobile IPv6 provides the possibility for the mobility of the IP layer, it can assign a permanent global IP address to each communication device, and can realize the connection between any point in the global area.

1.4 IPv6 address cost is relatively low

Currently, the secondary market transfer price of IPv4 addresses is about $15 per address. And for most governments, enterprises and home users, basically can get a large number of IPv6 addresses without any cost, so even in the face of the need to use a lot of IPv6 address enterprise cloud, government cloud and other deployment planning, its IP address cost is low.

2. Analysis of the status quo of ipv6-oriented carrier security system

Although China began to apply IPv6 in the three major operators in 2018, after the construction of talent teams, management system reform, and development of technical means in recent years, the operators basically have a relatively perfect network security guarantee system, and have also established a unified security management platform and system in order to better implement the relevant regulatory requirements. However, there are still some problems:

On the one hand, since the introduction of IPv6, the network architecture has undergone a series of evolution and changes: the service system needs to realize cross-domain connection; Various IT systems and their related platforms need to merge and merge; Network security operation and maintenance systems should also be affected by this and adjusted in a timely manner. In the face of so many changes, the network security operation and maintenance area has expanded, which is prone to problems such as blurred security protection boundaries and mixed deployment of services, and simply relying on the current security equipment guarantee means can not meet the actual needs of network security operation and maintenance. On the other hand, with the continuous application of IPv6, the majority of users' communication equipment will inevitably have a higher information release capability in the future, and will be exposed to the Internet in large numbers, but the existing security system has not been able to fully cope with large-scale attacks on user assets, network terminals are maliciously used and other security events.

All in all, from the above two aspects, for IPv6, our existing carrier security system in technology, management, personnel and many other aspects have certain deficiencies.

3. IPv6 oriented carrier security system reconstruction planning

3.1 Ensure the security and reliability of IPv6 network basic resource services

First of all, it is necessary to have real and reliable IP addresses. Generally, IPv4 networks generally use NAT44 and private network addresses, which is prone to the problem that IP addresses are difficult to control and cannot be traced to the source, resulting in a series of security risks. The IPv6 network uses the real IPv6 address, which greatly eliminates the uncontrollable and unreliable factors of the address. Therefore, to actively promote the IPv6 address real-name system and ensure that the address is traceable and traceable, can provide a safe and reliable environment foundation for IPv6 network.

Secondly, a reliable domain name management system should be established. Especially for the domain names of some important information systems, we must use the top-level domain name and its resolution system which is more in line with the characteristics of our country's independent management and control, so as to avoid security risks in the process of domain name resolution as much as possible.

Finally, there must be a DNS service with high credibility. In total, there are 13 global root DNS servers on the IPv4 network, but none of them are based in China. Especially from the current point of view, the global Internet management mechanism is not perfect, in this case, we do have a certain risk problems need to strengthen prevention. In this context, "Yeti Project" launched the IPv6 root server system, which not only provides a new choice for the majority of network users to use DNS, but also provides the Internet with "DNS disaster recovery emergency service" guarantee. In this way, even if some accidents occur in the global root DNS service, China's Internet can still operate and maintain and manage normally, which can more effectively avoid the occurrence of huge losses caused by Internet accidents.

3.2 To establish an IPv6 network security protection system as a whole

In the past decades, the government, enterprises and all walks of life have gradually established a series of security management subsystems, such as identity management, secure access and threat management, in their respective information construction, combined with their own actual needs and security issues. With the continuous development of trusted network thinking, network users should actively open up the channels between various security subsystems, and establish a reliable IPv6 network security protection system through mutual cooperation, so as to improve the overall security defense capability of the Internet. From the current development trend, the IPv6 network era is bound to completely change the shape and structure of the IPv4 network era, but in the face of such large-scale IPv6 address resources, Internet of Things devices, DNS attack and data security, intelligent terminal protection is bound to usher in a lot of new security problems. For these new problems, it is more necessary for us to establish a secure and credible IPv6 network security protection system, as far as possible from the perspective of practical application scenarios combined with IPv6 network characteristics to design and deploy related problem solutions, and ensure that the programs run simultaneously, so as to truly ensure the security and stable operation of the new IPv6 network information system.

3.3 It is necessary to continuously improve the monitoring and handling capacity of IPv6 network upgrade

When carrying out the IPv6 supporting upgrade work of various security systems, we should not only do a good job of IPv6 traffic support transformation work, but also actively expand the threat characteristics related to IPv6 network, but also pay attention to the completion of the upgrade work, and actively carry out normal operation monitoring and management. For traffic platforms, IPv6 application security in user networks such as the industrial Internet and the Internet of Things should be strengthened, so as to realize the detection and protection of IPv6 full traffic. And for the internal systems that need to be transformed to support IPv6 (such as internal operation management, office network, etc.), it is necessary to do a good job in the process of upgrading and upgrading, to ensure that the security protection equipment can support and enable IPv6 network security protection in accordance with actual needs at the same time. In addition, we also have to pilot in the home gateway, 5G network, MAN and other infrastructure networks, trying to use IPv6 firewall, gateway access control and a series of protective means to avoid the majority of network users' assets under attack or malicious use.

3.4 We should strengthen the filing management of IPv6 network security level protection

From the current point of view, the grading record and other requirements in the grade protection have not specifically formulated specific rules for IPv6 networks, so in the process of its practical application, it is often prone to the problem of inconsistent format and inconsistent standards. Therefore, we should add special inspection items about IPv6 network in the internal security inspection, and timely rectification and optimization of the weak links and existing problem risks found, and then carry out risk assessment on IPv6 network, and according to the evaluation results of the classification of the record, in order to strengthen the security level protection of IPv6 network record management. In addition, we should actively explore the methods and paths of IPv6 network real-name system, so as to provide convenience and basic guarantee for the follow-up security operation and grade protection filing management, in order to reduce the capital cost of later transformation and upgrading.

3.5 To combine the characteristics of IPv6 network and security needs to develop products

In order to further promote the reconstruction and planning of the security system of operators, we need to focus on the IPv6 network security products of operators, and actively transform and audit them, so as to do a good job in the industrial chain coordination. On the one hand, we should increase the research and analysis of new IPv6 scenario service types and new traffic models and their regulatory requirements analysis, so as to understand the challenges brought by ipv6-oriented carrier security system and find specific solutions, so as to improve the product's autonomous and controllable security capabilities. On the other hand, we should combine the characteristics of IPv6 network and its security requirements, try to develop and apply a variety of security technology products, such as cyberspace asset mapping, threat depth detection, security capability management platform, etc., so as to further promote the national and industrial IPv6 network security capability building. In addition, in addition to the research and development and application of these security technology products, we also have to actively innovate in the process of IPv6 security construction and operation and maintenance practice, and learn

from experience by participating in various pilot demonstration projects, so as to provide a scientific basis for the improvement of security technology products.

3.6 To strengthen the training of IPv6 network security personnel

Talent is the core resource for reconstructing and planning IPv6 network operators' security guarantee system. After all, all work is carried out by people, and all security accidents are also human problems in the final analysis. Therefore, if we want to build a secure and credible IPv6 network, we must strengthen the security training and education of IPv6 network technology and knowledge and technology training, and cultivate a group of high-quality and high-level IPv6 network security talents as far as possible. This is a key element for China to further promote IPv6 deployment planning, promote IPv6 network evolution and upgrading, and it is also the basic guarantee for China to truly realize the strategic planning of network power.

4. Concluding Remarks

To sum up, with the continuous enrichment of IPv6+ applications and the rapid increase of traffic, the security guarantee system of operators will certainly face more new challenges in the future. Therefore, it is necessary for us to build a set of IPv6 network security protection system with "endogenous security, defense in depth" network characteristics, so as to provide guarantee for the security operation and maintenance of national IPv6 network technology.

References:

[1] Hang Cui,Huan Li,Congguo She,Tong Mao. From "building" to "using" China's IPv6 development trend and telecom operator strategy recommendations [J]. Communication Enterprise Management, 2022 (07): 10-13.

[2] Jia Liu,Hongxiao Shi,Yu Li. Research on intelligent Cloud network Solution for operators in IPv6+ era [J]. Communications and Information Technology,2022(03):71-74.

[3] Yongyi Wu. Opportunities and Challenges coexist for promoting IPv6 scale deployment and application operators [N]. Communication Information Journal,2022-05-11(004).